Practical Free-Space Quantum Key Distribution

W. T. Buttler, R. J. Hughes, P. G. Kwiat, S. K. Lamoreaux, G. G. Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson, and C. M. Simmons (P-23)

Introduction

Quantum cryptography was introduced in the mid-1980s[1] as a new method for generating the shared, secret random number sequences, known as cryptographic keys, that are used in cryptosystems to provide communications security. Existing methods of key distribution derive their security from the perceived intractability of certain problems in number theory (which grow more vulnerable as computers grow more powerful), or from the physical security of the distribution process (which often depends upon couriers, increasing the likelihood that the key might be compromised). The appeal of quantum cryptography is that its security is based on the natural laws governing the behavior of photons, laws that solidly guard against the possibility of successful eavesdropping and interception.

In past years, our team has played a major role in demonstrating that quantum key distribution (QKD) is possible over multikilometer distances of optical fiber.[2, 3, 4] Free-space QKD, however, presents a greater challenge. The success of free-space QKD depends on the ability to transmit and detect single photons against a high background (that is, interference from other photon sources) and through a turbulent medium (the air). Building on previous efforts to demonstrate free-space QKD[5,6] we have developed and successfully tested a QKD system over an outdoor free-space optical path of close to 1 km under nighttime conditions. Our results, which were reported in *Physical Review Letters*[7], show that free-space QKD can provide secure, real-time key distribution between parties who need to communicate secretly. This has definite practical advantages over fiber optic systems, making QKD a viable alternative for secure surface-to-satellite communications.

Demonstration and Results

The QKD transmitter in our demonstration (Fig. 1) consisted of a temperature controlled single-mode (SM) fiber pigtailed diode laser, a fiber to free-space launch system, a 2.5-nm bandwidth interference filter (IF), a variable optical attenuator, a polarizing beam splitter (PBS), a low-voltage Pockels cell, and a 27× beam expander. The diode laser wavelength was temperature-adjusted to 772 nm, and the laser was configured to emit a short pulse of approximately 1-ns duration, containing ~10^5 photons.

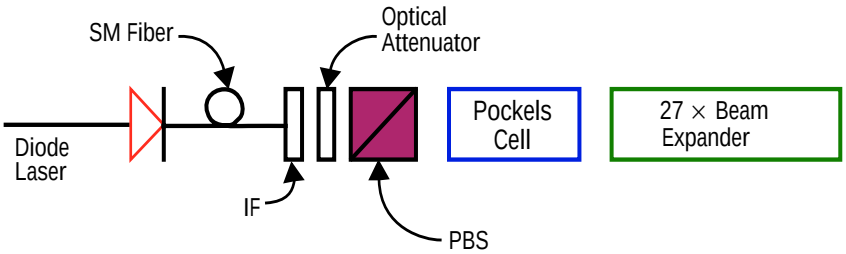

Fig. 1 Diagram of our free-space QKD transmitter.

In our QKD system, the sender, "Alice," starts by generating a secret random binary number sequence. Using a computer control system, Alice pulses the laser at a rate previously agreed upon between herself and the recipient, "Bob." Each laser pulse is launched into free space through the IF, and the pulse is then attenuated to an average of less than one photon per pulse, based on the assumption of a statistical Poisson distribution. The photons that are transmitted by the optical attenuator are then polarized by the PBS. Alice and Bob agree in advance on the polarization states that she will send, as well as those he will measure; their algorithm can be shared with the public without threatening the security of the system. In our demonstration, we used the B92 protocol.[8] The PBS was set to transmit an average of less than one horizontal-polarized photon, $|h\rangle$, to the Pockels cell, and the Pockels cell was then randomly switched to either pass the light unchanged as $|h\rangle$ (zero-wave retardation) or change it to a right-circular-polarized photon, $|r\rangle$ (quarter-wave retardation).

The QKD receiver in our demonstration (Fig. 2) used an 8.9-cm Cassegrain telescope to collect the photons and direct them to the receiver optics and detectors. The receiver optics consisted of a 50/50 beam splitter (BS) that randomly directed the photons onto either of two distinct optical paths, each of which measures for one of the agreed-upon polarization states. One output port along each optical path was coupled by multimode (MM) fiber to a single-photon counting module (SPCM). Although the receiver did not include IFs, the spatial filtering provided by the MM fibers effectively reduced ambient background noise during nighttime operation (~1.1 kHz) to negligible levels. The lower optical path contained a polarization controller (a quarter-wave retarder and a halfwave retarder) followed by a PBS to test collected photons for $|h\rangle$; the upper optical path contained a half-wave retarder followed by a PBS to test for $|r\rangle$.

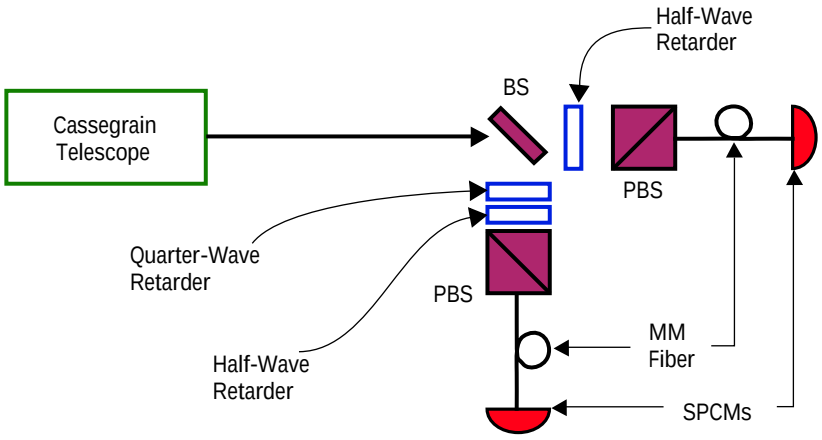

Fig. 2 Diagram of our free-space QKD receiver.

Note that Bob does not look for Alice's original states, but for related states. This ensures that Bob will never detect a photon for which he and Alice have used a preparation/measurement pair that corresponds to different bit values, which happens for 50% of the bits in Alice's sequence. For example, a single |*r*> photon traveling along the lower path encounters the polarization controller and is converted to |*v*> and reflected away from the SPCM by the PBS. Conversely, a single |*h*> photon traveling the same path is converted to |*r*> and transmitted toward or reflected away from the SPCM in this path with equal probability. Similarly, a single |*h*> photon traveling the upper path encounters a half-wave retarder and is converted to |*v*> and is reflected away from the SPCM in this path, but a single |*r*> photon traveling this path is converted to a left-circular-polarized photon, |*l*>, and transmitted toward or reflected away from the SPCM with equal probability. Thus, by detecting single photons, Bob identifies only a random 25% portion of the bits in Alice's random bit sequence, assuming a single photon Fock state with no bit loss in transmission or detection. This 25% efficiency factor is the price that Alice and Bob must pay for secrecy.

To complete the QKD procedure, Bob and Alice reconcile their common bits through a public discussion by revealing the locations, but not the bit values, in the sequence where Bob detected photons; Alice retains only those detected bits from her initial sequence. The resulting detected bit sequences comprise the raw key material from which a pure key is distilled using classical error detection techniques. Once Alice and Bob share this unique key, they can code, transmit, and decode messages securely.[7]

In our demonstration, we operated the transmitter and receiver optics over 240-, 500-, and 950-m outdoor optical paths under nighttime conditions with the transmitter and receiver collocated to simplify data acquisition. All optical paths were achieved by reflecting the emitted beam from a 25.4-cm mirror positioned at the halfway point of the transmission distance.

Results for the 950-m path showed a bit error rate (BER), defined as the ratio of the bits received in error to the total number of bits received, of ~1.5% when the system was operating at a level of ~0.1 photons per pulse (BERs of ~0.7% and ~1.5% were observed for the 240-m and 500-m optical paths, respectively). A sample of raw key material from the 950-m test, including errors, is shown in Fig. 3. Using narrow gated coincidence timing windows (~5 ns) and spatial filtering, we minimized the bit errors due to ambient

Sender's raw key:
11111110000001010101101111110011111101111010100110100101110111
Receiver's ray key:
11111*0*1000000101010110111111000*1*111101111010100110100101110111

Fig. 3 A sample of the sender's and receiver's raw key material, which was generated in our demonstration across a free-space distance of ~1 km. Only two errors, indicated in red, occurred during this transmission.

background to less than ~1 every 9 seconds. Further, because detector dark noise (~80 Hz) contributed only about one dark count every 125 seconds, we believe that the observed BER was mostly caused by misalignment and imperfections in the optical elements (wave plates and Pockels cell). While this BER surpasses even the BER attained with our fiber systems[2,3,4], any BER may potentially be caused by an eavesdropper. "Privacy amplification" must therefore be applied.[9]

Toward QKD for Satellite Communications

One of the goals of our demonstration was to evaluate the feasibility of conducting free-space QKD between a ground station and a satellite in a low-earth orbit. We designed our QKD system to operate at a wavelength of 772 nm, at which the atmospheric transmission from surface to space can be as high as 80%, and for which single-photon detectors with efficiencies as high as 65% are commercially available; at these optical wavelengths, atmospheric depolarizing effects are negligible, as is the amount of Faraday rotation experienced on a surface-to-satellite path.

To detect a single QKD photon it is necessary to know when it will arrive. The photon arrival time can be communicated to the receiver by using a bright precursor reference pulse. Received bright pulses allow the receiver to set a 1-ns time window within which to look for the QKD photon. This short time window reduces background photon counts dramatically. Background can be further reduced by using narrow bandwidth filters.

Atmospheric turbulence introduces beam wander, impacting the rate at which QKD photons would arrive at a satellite from a ground-station transmitter. The optical influence of turbulence is dominated by the lowest ~2 km of the atmosphere, the region in which our demonstration was conducted; the results of our 1-km experiment provide strong evidence that surface-to-satellite QKD will be feasible.

Assuming 30-cm diameter optics at both the transmitter and satellite receiver[7] and worst-case atmospheric "seeing" of 10 arc-seconds, we estimate that with a laser pulse rate of 10 MHz, an average of one photon per pulse, and atmospheric transmission of ~80%, photons would arrive at the collection optic at a rate of 800 to 10,000 Hz. Then, with a 65% detector efficiency, the 25% intrinsic efficiency of the B92 protocol, IFs with transmission efficiencies of ~70%, and a MM fiber collection efficiency of ~40%, a key generation rate of 35–450 Hz is feasible. With an adaptive beam tilt corrector, the key rate could be increased to about 3.5–45 kHz; these rates would double using the BB84 protocol.

Another challenge for surface-to-satellite QKD is the influence of ambient background. From our preliminary estimates of background photon rates during the full moon and new moon, we infer BERs of $\sim 9 \times 10^{-5}$ to 9×10^{-3} and $\sim 2 \times 10^{-6}$ to 3×10^{-5}, respectively. During daytime orbits the background radiance will be ~1% larger. We have recently demonstrated point-to-point, free-space QKD in daylight conditions. Results from initial tests have been positive, promising solutions to the challenge of distinguishing the single-photon signal in a bright background.

Already, our results show that QKD between a ground station and a low-earth orbit satellite should be possible on nighttime orbits, and possibly even in full daylight. During the several minutes that a satellite would be in view of the ground station there would be adequate time to generate tens of thousands of raw key bits, from which a shorter error-free key stream of several thousand bits would be produced after error correction and privacy amplification. If our tests in daylight conditions prove successful, it will remove the last great obstacle to this technology, ensuring that the promise of secure, surface-to-satellite communications becomes a reality.

References

[1] C. H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), p. 175.

[2] R. J. Hughes, D. M. Alde, P. Dyer, G. G. Luther, G. L. Morgan, and M. Schauer, "Quantum Cryptography," *Contemporary Physics* 36, 149 (1995).

[3] R. J. Hughes, *et al.*, "Quantum Cryptography Over Underground Optical Fibers," *Lecture Notes Computational Science* 1109, 329 (1996).

[4] R. J. Hughes, "Secure Communications using Quantum Cryptography," *SPIE Proceedings* 3076, 2 (1997).

[5] W. T. Buttler, R. J. Hughes, P. G. Kwiat, G. G. Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson, and C. M. Simmons, "Free-Space Quantum-Key Distribution," *Physical Review A* 57, 2379 (1998).

[6] B. C. Jacobs and J. D. Franson, "Quantum Cryptography in Free Space," *Optical Letters* 21, 1854 (1996).

[7] W. T. Buttler, R. J. Hughes, P. G. Kwiat, S. K. Lamoreaux, G. G. Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson, and C. M. Simmons, "Practical Free-Space Quantum Key Distribution Over 1 km," *Physical Review Letters* 81, 3283 (1998).

[8] C. H. Bennett, "Quantum Cryptography using any Two Nonorthogonal States," *Physical Review Letters* 68, 3121 (1992).

[9] C. H. Bennett, *et al.*, "Generalized Privacy Amplification," *IEEE Transactions on Information Theory* 41, 1915 (1995).